УДК:004.056.5

Е.В. Каверина, Е.В. Ромашка

БЕЗОПАСНОСТЬ WEB-РЕСУРСОВ. УЯЗВИМОСТИ В СТЕКЕ ПРОТОКОЛОВ TCP/IP.DOS АТАКИ

Важность построения системы информационной безопасности подтверждается постоянным ростом хакерских атак, нападений на банковские, корпоративные сети и компьютеры частных пользователей. Многие современные информационные системы создаются в виде web-сайтов, поэтому безопасность веб-приложений — одна из наиболее актуальных тем в контексте информационной безопасности.

Основой работы сети Интернет является набор (стек) протоколов TCP/IP (Transmission Control Protocol/Internet Protocol), уязвимостями которого часто пользуются злоумышленники. Эти уязвимости обусловлены, как правило, слабой аутентификацией, лимитированием масштаба буфера, неимением проверки правильности информации и т.п. В последнее время одним из самых распространённых типов атак являются, так называемые, DoS-атаки.

Отказ в обслуживании или Denial of Service (DoS) атака на вычислительную систему с целью нарушения доступности некого информационного актива. Если атака проводится для множества сетевых устройств, говорят о распределенной атаке DoS (DDoS - distributed DoS), она намного опаснее своей единичной версии и используется чаще всего. Для DDoS атак обычно используются целые сети поддельных клиентов сайта. Основной опасностью подобных атак является потеря прибыли. Сегодня чаще всего можно встретить следующие пять разновидностей DoS-атак: smurf - ping-запросы ICMP. Злоумышленник посылает постоянный поток ping-пакетов по широковещательному адресу. Все устройства, получив запрос, отвечают отправителю пакетом ICMP ECHO REPLY; ICMP flood – атака, такая же, как и Smurf, только без усиления,

создаваемого запросами; UDP flood - отправка на адрес атакуемого узла множества пакетов UDP (User Datagram Protocol); TCP flood - отправка на адрес атакуемого узла множества TCP-пакетов; TCP SYN flood - при проведении такого рода атаки выдается большое количество запросов на инициализацию TCP-соединений с атакуемым узлом.

В основном для защиты используются превентивные меры для предотвращения атак, такие как: увеличение полосы пропускания, создание виртуальной серверной инфраструктуры в нескольких центрах данных, настройка маршрутизаторов для предотвращения DDoS-атаки пингования, приобретение специализированных аппаратных и программных средств у соответствующих вендоров, защита DNS-серверов и их распределение. Если атака всё же началась необходимо чётко понимать, как ей противодействовать. Есть несколько мер, которые предназначены для частичного ослабления атаки: ограничение скорости маршрутизатора, установка на него фильтров и определённых условий сброса пакетов, установление таймаута на полуоткрытые соединения.

Для единичного пользователя DoS и DDoS атаки не столь опасны ввиду того, что они не предоставляют злоумышленникам доступ к персональным данным как фишинг или возможность удаления и изменения фалов как разнообразные вредоносные программы. Однако крупным компаниям они могут принести большие убытки и, к сожалению, универсальной защиты от подобных атак не существует, а остановить уже начавшуюся атаку гораздо сложнее чем предотвратить её появление. Поэтому защите от DDoS-атак необходимо постоянно уделять самое пристальное внимание.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Браун, С. “Мозаика” и “Всемирная паутина” для доступа к Internet: Пер. с англ. - М.: Мир: Малип: СК Пресс, 1999. - 167с.

2. Кочерян, Р. Схема инета // Спец Хакер. - 2002. - №11 – С.4-9.

3. DDoS-атаки. Причины возникновения, классификация и защита от DDoS-атак [Электронный ресурс]. URL: http://efsol.ru/articles/ddos-attacks.html

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПБ.: Питер, 2010. – 944 с.:ил.